IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF MICHIGAN

JOHN SCOTT SMITH, individually and on behalf of all others similarly situated, Plaintiff, v. FLAGSTAR BANCORP, INC. and FLAGSTAR BANK, FSB, Defendant.	Case No.: **JURY TRIAL DEMANDED**

CLASS ACTION COMPLAINT

Plaintiff John Scott Smith ("Plaintiff"), by and through the undersigned counsel, brings this class action complaint against Defendant Flagstar Bancorp, Inc. and Flagstar Bank, FSB (collectively, "Defendant" or "Flagstar"), on behalf of himself and all others similarly situated. Plaintiff makes the following allegations based upon personal knowledge as to his own actions and upon information and belief as to all other matters.

NATURE OF THE CASE

1. Plaintiff brings this class action against Flagstar for its failure to secure and safeguard consumers' personally identifiable information ("PII")[1] and for failing

[1] PII is information that is used to confirm an individual's identity, and in this instance includes an individual's name and Social Security number.

to provide timely, accurate, and adequate notice to Plaintiff and Class Members that their PII had been stolen.

2. On June 17, 2022, Flagstar, a Michigan-based bank and mortgage lender that operates more than 150 branches nationwide, published a notice on its website stating that it was the subject of a massive data breach whereby hackers gained unauthorized access to its networks between December 3 and December 4, 2021, affecting over 1.5 million U.S. customers (the "Data Breach").

3. Flagstar admits the hackers were able to access and exfiltrate highly-sensitive information stored on Flagstar's servers, including customers' full names and Social Security numbers. Flagstar admits that PII for approximately 1.5 million United States customers were accessed during the Data Breach.

4. Flagstar discovered the unauthorized access in December 2021, but failed to inform the public of the Data Breach until almost six months later.

5. The Data Breach occurred because Flagstar failed to implement reasonable security procedures and practices, failed to disclose material facts surrounding its deficient data security protocols, and failed to timely notify the victims of the Data Breach.

6. As a result of Flagstar's failure to protect the sensitive information it was entrusted to safeguard, Plaintiff and Class Members did not receive the benefit of their bargain with Flagstar and now face a significant risk of identity theft and

fraud, financial fraud, and other identity-related fraud now and into the indefinite future.

PARTIES

7. Defendant Flagstar Bancorp, Inc. is a corporation formed in Michigan with its principal place of business located at 5151 Corporate Drive, Troy, Michigan 48098.

8. Defendant Flagstar Bank, FSB is a Michigan-based, federally chartered stock savings bank with its corporate headquarters located at 5151 Corporate Drive, Troy, Michigan 48098.

9. Plaintiff John Scott Smith is a resident of National City, California in San Diego County, California. Plaintiff Smith was a customer of Flagstar and a victim of the Data Breach.

JURISDICTION AND VENUE

10. This Court has subject matter jurisdiction over this action pursuant to the Class Action Fairness Act of 2005, 28 U.S.C. § 1332(a) and (d), because the matter in controversy, exclusive of interest and costs, exceeds the sum or value of five million dollars ($5,000,000.00), there are more than 100 proposed Class Members and minimal diversity exists as Defendant is a citizen of States different from that of at least one Class Member. This Court also has supplemental jurisdiction

pursuant to 28 U.S.C. § 1367(a) because all claims alleged herein form part of the same case or controversy.

11. The Court has personal jurisdiction over Flagstar because Flagstar headquartered in this District and is authorized to and regularly conducts business in the State of Michigan. Flagstar sells, markets, and advertises its products and services to Plaintiff and Class Members located in the State of Michigan and, therefore, has sufficient minimum contacts to render the exercise of jurisdiction by this Court proper and necessary.

12. Venue is proper in this judicial district pursuant to 28 U.S.C. § 1391 because Flagstar has a principal place of business in this district; Flagstar transacts substantial business, has agents, and is otherwise located in this district; and a substantial part of the conduct giving rise to Plaintiff's claims occurred in this district.

FACTUAL ALLEGATIONS

Flagstar's Privacy Practices

13. Flagstar operates over 150 branches in areas including Indiana, California, Wisconsin, and Ohio, and its mortgage divisions operate nationally through 82 retail locations.[2] Flagstar is one of the largest banks in the United States, having total assets of over $23.2 billion and generating annual revenues in excess of

[2] https://www.flagstar.com/about-flagstar.html (last visited June 28, 2022).

$1.6 billion.[3] Flagstar describes itself as the sixth-largest bank mortgage originator nationally.[4]

14. In the course of providing financial services, Flagstar collects highly sensitive PII, such as Social Security numbers, from its customers. As a result, when customers use Flagstar's services, their highly-sensitive PII is stored on centralized servers maintained by Flagstar.

15. Flagstar maintains a privacy policy dated February 2018 that is accessible from its website ("Privacy Policy"). The Privacy Policy describes the circumstances in which Flagstar collects the personal information of its customers:

> We collect your personal information, for example, when you:
>
> - Open an account or deposit money
> - Pay your bills or apply for a loan
> - Use your debit card
>
> We also collect your personal information from others, such as credit bureaus, affiliates, or other companies.[5]

16. Flagstar's Privacy Policy includes a section entitled: "How does Flagstar Bank protect my personal information?" Flagstar answers this question representing as follows: "To protect your personal information from unauthorized

[3] https://www.infosecurity-magazine.com/news/us-bank-data-breach-impacts-15/ (last visited June 28, 2022).
[4] https://www.flagstar.com/about-flagstar.html (last visited June 28, 2022).
[5] https://www.flagstar.com/content/dam/flagstar/pdfs/about-flagstar/PrivacyPolicy.pdf (last visited June 28, 2022).

access and use, we use security measures that comply with federal law. These measures include computer safeguards and secured files and buildings."[6]

17. Given the amount and sensitive nature of the data it collects and recognizing that "[r]apid advances in technology and creative criminal minds make fraud a potentially serious threat on a variety of fronts,"[7] Flagstar also maintains a "Fraud Information Center," and claims the company is "continually taking steps to reduce the instances of fraud" for consumers,[8] and has "built processes to identify cybersecurity threats and ensure our data and customer privacy are well-protected."[9] Flagstar represents to its customers that it employs "firewalls and prevention systems that stop unauthorized access to our network and computers."[10]

18. By obtaining, collecting, and storing the PII of Plaintiff and Class Members, Defendant assumed legal and equitable duties and knew or should have known it was responsible for protecting the PII from unauthorized disclosure.

---

[6] *Id.*
[7] https://www.flagstar.com/fraud-information-center/preventing-fraud.html (last visited June 28, 2022).
[8] *Id.*
[9] https://www.flagstar.com/esg/governance/data-security-and-customer-privacy.html (last visited June 28, 2022).
[10] https://www.flagstar.com/fraud-information-center/preventing-fraud.html (last visited June 28, 2022).

The Data Breach

19. Between December 3 and December 4, 2021, hackers infiltrated Flagstar's corporate network and accessed a treasure trove of highly sensitive customer information stored on its servers, including full names and Social Security numbers for 1.5 million customers.

20. Flagstar did not disclose the existence of the Data Breach until almost six months later. In an official press release posted to Flagstar's website on June 17, 2022, Flagstar publicly acknowledged the Data Breach for the first time, vaguely stating that "Flagstar experienced a cyber incident that involved unauthorized access to our network" in December 2021.[11]

21. Under the press release's section titled "What happened?" Flagstar provides consumers with no meaningful detail regarding the Data Breach—omitting any detail regarding the Data Breach's cause, scope, or impact; the timeline of the investigation into the breach; or the remedial measures taken to ensure customers' data security moving forward. Instead, Flagstar downplays the Data Breach in broad terms: "Upon learning of the incident, we promptly activated our incident response plan, engaged external cybersecurity professionals experienced in handling these types of incidents, and reported the matter to federal law enforcement. We continue

[11] https://www.flagstar.com/customer-support/customer-data-information-center.html (last visited June 28, 2022).

to operate all services normally. Since then, we have taken several measures to toughen our information security. We now believe we have strengthened our cyber vulnerabilities in the future."[12]

22. Under the press release's section titled "What is Flagstar doing?" Flagstar claims it concluded an "extensive forensic investigation and manual document review" on June 2, 2022. Flagstar provides no information regarding when this investigation commenced; what it entailed; what it found; or why Flagstar hid the investigation from customers for, ostensibly, months.

23. Similar in content to its dedicated webpage, the data breach notification letters Flagstar sent to the victims of its Data Breach provide little additional detail regarding what occurred.[13] Describing the Data Breach as a "recent security incident," Flagstar states the Data Breach "involved unauthorized access to our network" but provides no details on who accessed the network, how they did so, or the type of PII potentially accessed. Flagstar further states that "[u]pon learning of the incident, we promptly activated our incident response plan" and [a]fter an extensive forensic investigation and manual document review, we discovered on June 2, 2022 that certain impacted files containing your personal information were

[12] *Id.*

[13] https://www.documentcloud.org/documents/22064071-flagstar-standard-notification-letter-06-17-2022?responsive=1&title=1 (last accessed June 27, 2022).

accessed and/or acquired from our network between December 3, 2021 and December 4, 2021."

24. The letter offers empty assurances that Flagstar has "no evidence that any of the information has been misused," but makes no effort to explain what efforts Flagstar undertook to come to that conclusion. In reality, this statement is self-serving and meaningless: Flagstar necessarily would not receive reports of PII misuse from its customers until *after* Flagstar notified victims that their PII had been stolen in the Data Breach; put differently, customers would not be able to trace identity theft or fraud to Flagstar's Data Breach until Flagstar disclosed the Data Breach to them. Flagstar included this disingenuous and facially dubious statement in its letter to downplay the substantial fraud risk faced by the victims of its Data Breach.

25. Notwithstanding, Flagstar tacitly admits that victims are at risk of harm by advising them to take certain actions like monitoring their financial accounts and "placing a fraud alert and/or security freeze on your credit files" to "help protect your personal information." Flagstar also offered victims two years of credit monitoring services "out of an abundance of caution."

26. Flagstar provides no explanation for why it delayed notifying customers about the Data Breach for almost six months after the Data Breach occurred and 15 days after it allegedly concluded its investigation. By waiting

months to disclose the Data Breach and by downplaying the risk that victim's PII would be misused by bad actors, Flagstar prevented victims from taking meaningful, proactive, and targeted mitigation measures to protect themselves from harm.

Flagstar's Previous Security Troubles

27. This is the second major incident to impact Flagstar and its customers in a year. In January 2021, a notorious hacking group breached the servers of Flagstar's vendor, Accellion, and accessed the customer data of 1.48 million Flagstar employees and customers.

28. This breach resulted in Flagstar being extorted by Clop, its customers having their data exposed to cybercriminals, and the financial institute ending its collaboration with the Accellion platform.

29. After Flagstar began notifying victims of the data breach starting in March of 2021, the hacking group released screenshots of stolen personal data including Social Security numbers, names, addresses, phone numbers, and tax records—with a warning that it had stolen a lot more.

30. Flagstar was named as a defendant in five separate putative class actions relating to the breach and ultimately settled those cases in late 2021.

The Data Breach was Preventable

31. In response to the Data Breach, Flagstar stated it has "taken several measures to toughen our information security" and that it "now believe[s] we have

strengthened processes and systems in a way that should reduce our cyber vulnerabilities in the future."[14]

32. But Flagstar, like any financial services provider its size storing valuable data, should have had robust protections in place to detect and terminate a successful intrusion long before access and exfiltration could expand to millions of customer files. Flagstar's implementation of enhanced security measures only after the fact is inexcusable given its knowledge that it was a prime target for cyberattacks.

33. To be sure, the financial services industry is frequently one of the most targeted sectors for cyberattacks because of the information financial services providers collect and store, including financial and personal information of customers—all extremely valuable on underground markets.[15] A 2016 Financial Cybersecurity Report by SecurityScorecard revealed that 75% of the leading banks in the United States are infected with malware, and approximately one in five financial institutions uses email service providers with "severe security vulnerabilities."[16]

[14] https://www.flagstar.com/customer-support/customer-data-information-center.html (last accessed June 27, 2022).
[15] https://www.forbes.com/sites/forbesfinancecouncil/2022/03/09/for-financial-institutions-cyberthreats-loom-large/?sh=69dd96d82ddb (last visited June 28, 2022).
[16] https://www.helpnetsecurity.com/2016/08/05/us-banks-malware/ (last visited June 28, 2022).

34. Its status as a prime target for cyberattacks was known and obvious to Flagstar as it observed frequent public announcements of data breaches affecting financial services providers and knew that information of the type it collected, maintained, and stored is highly coveted and a frequent target of hackers.

35. To state a few examples: in 2017, Equifax suffered a breach in which the personal data of more than 147 million consumers was exposed. In March 2019, Capital One suffered from a data breach affecting approximately 106 million individuals in the United States and Canada, following a series of three other data breaches in preceding years.[17] In 2019, Centerstone Insurance and Financial Services experienced a phishing campaign that allowed hackers to exfiltrate data of over 100,000 consumers. On December 24, 2019, researchers discovered a data breach from Advantage and Argus Capital Funding, a NY-based private equity firm, which included 425GB of 500,0000 legal and financial documents including Social Security information.[18] On July 25, 2020, hackers published data and personal information of 7.5 million users of the "Dave" banking application, including full names and Social Security numbers.[19] American Express, SunTrust Bank, and Discover have each experienced more than four data breaches a piece dating back to

[17] Bitglass_Financial_Matrix2019.pdf (last visited June 28, 2022).
[18] https://carnegieendowment.org/specialprojects/protectingfinancialstability/timeline#click-hide (last visited June 28, 2022).
[19] *Id.*

2006.[20] These represent a fraction of the data breaches affecting the financial services sector, of which Flagstar was or should have been aware.

36. A report compiled from data by the Identity Theft Resource Center reveals that the financial services industry contributed 62% of exposed data, accounting for 6.5% of data breaches in 2019.[21]

37. According to the Identity Theft Resource Center, the financial services sector accounted for 15.5% of data breaches in Q3 of 2021.[22]

38. According to the Verizon 2021 Data Breach Investigations Report, "96% [of] breaches in the financial services industry were financially motivated."[23] And Federal Reserve Chairman Jerome Powell "warned last year that cyberattacks are the No. 1 threat to the global financial system."[24] "In fact, Cap Gemini's Top Trends in Banking 2022 declared cybersecurity is becoming a competitive differentiator for banks."[25] Indeed, cyber security attacks aimed at the banking sector "keep rising in frequency and intensity due to their high potential for payout."[26]

---

[20] 62% of breached data came from financial services in 2019 | CIO Dive (last visited June 28, 2022).
[21] 62% of breached data came from financial services in 2019 | CIO Dive (last visited June 28, 2022); Bitglass_Financial_Matrix2019.pdf (last visited June 28, 2022).
[22] If You're a Victim of a Data Breach | Northwest Bank (last visited June 28, 2022).
[23] *Id.*
[24] *Id.*
[25] *Id.*
[26] https://www.securitymagazine.com/articles/96128-banking-industry-sees-1318-

39. Bloomberg described the financial services sector's 2021 as an "unrelenting year of fighting off cyber threats," and warned financial services providers "should expect more of the same or even worse."[27] The Financial Services Information Sharing and Analysis Center's (FS-ISAC) annual report on cyber threats cited in the article, predicts "current trends to continue and possible worsen over the next year," stating cybersecurity is "no longer just a back-office cost."[28] These increases are "due to several factors," including the "rapid digitization of financial services, which accelerated during the pandemic," and "increased entry points for hackers to possibly exploit."[29] Teresa Walsh, who leads FS-ISAC's global intelligence office, described the financial sector as experiencing "a dizzying number of vulnerabilities."

40. According to Verizon's 2021 Data Breach Investigations Report, 30% of breaches in the financial and insurance industries were caused by web application attacks, primarily driven by external actors using stolen credentials to get access to sensitive data store in the cloud.[30] The Anti-Phishing Working Group (APWG) found that phishing attacks were most prevalent among financial institutions in Q1

---

increase-in-ransomware-attacks-in-2021 (last visited June 28, 2022).

[27] https://www.bloomberg.com/news/articles/2022-03-10/financial-firms-poised-for-worse-cyber-threats-after-trying-year (last visited June 28, 2022).

[28] *Id.*

[29] *Id.*

[30] https://www.verizon.com/about/news/verizon-2020-data-breach-investigations-report (last visited June 28, 2022).

of 2021.[31] And according to Akami's 2019 State of the Internet/Security Financial Services Attack Economy Report, 50% of all unique organizations impacted by observed phishing domains were from the financial services sector.[32]

41. At all relevant times, Flagstar knew, or reasonable should have known, of the importance of safeguarding PII and of the foreseeable consequences that would occur if its data security system was breached, including, specifically, the significant costs that would be imposed on its individual consumers as a result of a breach.

42. Flagstar was, or should have been, fully aware of the significant number of customers whose PII it collected, and thus, the significant number of customers who would be harmed by a breach of its systems.

43. But despite all of the publicly available knowledge of the continued compromises of PII and despite holding the PII of millions of customers, Flagstar failed to use reasonable care in maintaining the privacy and security of the PII of Plaintiff and Class Members. Had Flagstar implemented common sense security measures, hackers never could have accessed millions of customer files and the breach would have been prevented or much smaller in scope.

---

[31] https://www.upguard.com/blog/biggest-cyber-threats-for-financial-services#:~:text=Phishing%20Attacks%20increased%20by%2022,for%20the%20same%20comparative%20period. (last visited June 28, 2022).

[32] https://www.akamai.com/newsroom/press-release/state-of-the-internet-security-financial-services-attack-economy (last visited June 28, 2022).

Allegations Relating to Plaintiff John Smith

44. In approximately 2011, Plaintiff Smith obtained a home mortgage loan from Flagstar in connection with the purchase of a residential property in Bonita, California.

45. In connection with his application for a mortgage loan, Flagstar required Plaintiff Smith to provide financial and other highly sensitive personal information, including, among other things, his full name and Social Security number. At all relevant times, Flagstar stored Plaintiff Smith's PII on its internal servers.

46. In June 2022, Plaintiff Smith received a notification letter from Flagstar stating that he was a victim of the Data Breach. The letter stated: "we determined that one or more of the impacted files contained your social security number."

47. The letter recommended Plaintiff Smith take certain actions like monitoring his financial accounts, and "placing a fraud alert and/or security freeze on your credit files" to "help protect your personal information." The letter further asked Plaintiff Smith to "review the attachment to this letter, entitled 'Steps You Can Take to Help Protect Your Information,'" and to "remain vigilant in reviewing your financial account statements and credit reports for fraudulent or irregular activity on a regular basis."

48. Despite making these recommendations, Flagstar also attempted to downplay the risk of harm, stating in bold text: "**We have no evidence that any of your information has been misused**." This statement is facially dubious, as the objective of almost every data breach is to access information that can be misused for financial gain; and in any event, Plaintiff Smith would not be able to inform Flagstar of any misuse until *after* the company actually made him aware of the Data Breach.

49. As a result of the Data Breach, Plaintiff Smith has been the victim of extensive identity theft and fraud. In May 2022, Plaintiff Smith checked his bank account and realized there was a fraudulent $5,000 check negotiated from his account to an unknown third party. Plaintiff Smith had to sign an affidavit stating that the check was forged and he was advised by his bank to shut down his accounts. This was a long and arduous process as Plaintiff Smith maintained multiple accounts at the bank including two fiduciary accounts, a savings account, and a college account that had to be closed. This required Plaintiff Smith and his family members to take multiple trips to the bank to sign documents necessary to effectuate this process.

50. The following week, Plaintiff Smith attempted to pay a bill from his business account and realized he had a negative balance. He reviewed his recent transactions and realized that someone had accessed his account and issued

payments to credit cards that were not in his name. Again, Plaintiff Smith was forced to spend significant time and effort filling out fraud affidavits and taking steps to close the account, which he had maintained for his business for many years. In the process of closing the account, Plaintiff Smith learned that someone fraudulently attempted to negotiate a large check from the same account several weeks earlier, which was rejected due to insufficient funds.

51. To protect himself from additional harm, Plaintiff Smith took steps to change his account information at the other financial institutions where he maintained accounts and has been forced to spend significant time and effort engaging in remedial efforts to protect his finances from additional attacks. Plaintiff Smith must now continue to spend time and effort reviewing his financial account statements for evidence of unauthorized activity, which he will continue to do indefinitely. Plaintiff Smith suffered significant distress knowing his highly personal information is no longer confidential and his assets are being targeted.

52. Plaintiff Smith's last payment to Flagstar was in February 2021, at which time Plaintiff Smith sold his home and the customer relationship ended. Upon information and belief, Flagstar continues to store and/or share Plaintiff Smith's PII on its internal system. Thus, Plaintiff Smith has a continuing interest in ensuring that his PII is protected and safeguarded from future breaches.

Flagstar Failed to Comply with Federal Law and Regulatory Guidance

53. Defendant is a financial institution, as that term is defined by Section 509(3)(A) of the Gramm-Leach-Bliley Act (GLBA), 15 U.S.C. § 6809(3)(A), and thus is subject to the GLBA.

54. The GLBA defines a financial institution as "any institution the business of which is engaging in financial activities as described in Section 1843(k) of Title 12 [The Bank Holding Company Act of 1956]." 15 U.S.C. § 6809(3)(A).

55. Defendant collects nonpublic personal information, as defined by 15 U.S.C. § 6809(4)(A), 16 C.F.R. § 313.3(n), and 12 C.F.R. § 1016.3(p)(1). Accordingly, during the relevant time period, Defendant was subject to the requirements of the GLBA, 15 U.S.C. §§ 6801.1 *et seq.*, and is subject to numerous rules and regulations promulgated on the GLBA statutes.

56. The GLBA Privacy Rule became effective on July 1, 2001. *See* 16 C.F.R. Part 313. Since the enactment of the Dodd-Frank Act on July 21, 2010, the Consumer Financial Protection Bureau (CFPB) became responsible for implementing the Privacy Rule. In December 2011, the CFPB restated the implementing regulations in an interim final rule that established the Privacy of Consumer Financial Information, Regulation P, 12 C.F.R. § 1016 ("Regulation P"), with the final version becoming effective on October 28, 2014.

57. Accordingly, Defendant's conduct is governed by the Privacy Rule prior to December 30, 2011 and by Regulation P after that date.

58. Both the Privacy Rule and Regulation P require financial institutions to provide customers with an initial and annual privacy notice. These privacy notices must be "clear and conspicuous." 16 C.F.R. §§ 313.4 and 313.5; 12 C.F.R. §§ 1016.4 and 1016.5. "Clear and conspicuous means that a notice is reasonably understandable and designed to call attention to the nature and significance of the information in the notice." 16 C.F.R. §§ 313.3(b)(1); 12 C.F.R. § 1016.3(b)(1). These privacy notices must "accurately reflect[] [the financial institution's] privacy policies and practices." 16 C.F.R. § 313.4 and 313.5; 12 C.F.R. §§ 1016.4 and 1016.5. They must include specified elements, including the categories of nonpublic personal information the financial institution collects and discloses, the categories of third parties to whom the financial institution discloses the information, and the financial institution's security and confidentiality policies and practices for nonpublic personal information. 16 C.F.R. § 313.6; 12 C.F.R. § 1016.9. As alleged herein, Defendant violated the Privacy Rule and Regulation P.

59. Defendant failed to provide annual privacy notices to customers after the customer relationship ended, despite retaining these customers' PII and storing that PII on Defendant's network system.

60. Defendant further failed to adequately inform its customers that it was storing and/or sharing, or that it would store and/or share, the customers' PII on an insecure platform, accessible to unauthorized parties from the internet, and would do so after the customer relationship ended.

61. The Safeguards Rules, which implements Section 501(b) of the GLBA, 15 U.S.C. § 6801(b), requires financial institutions to protect the security, confidentiality, and integrity of customer information by developing a comprehensive written information security program that contains reasonable administrative, technical, and physical safeguards, including: (1) designating one or more employees to coordinate the information security program; (2) identifying reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of customer information, and assessing the sufficiency of any safeguards in place to control these risks; (3) designing and implementing information safeguards to control the risks identified through risk assessment, and regularly testing or otherwise monitoring the effectiveness of the safeguards' key controls, systems, and procedures; (4) overseeing service providers and requiring them by contract to protect the security and confidentiality of customer information; and (5) evaluating and adjusting the information security program in light of the results of testing and monitoring, changes to the business operation, and other relevant circumstances. 16

C.F.R. §§ 314.3 and 314.4. As alleged herein, Defendant violated the Safeguards Rule.

62. Defendant failed to assess reasonably foreseeable risks to the security, confidentiality, and integrity of customer information.

63. Defendant failed to adequately evaluate and adjust its information security program in light of the previous data breach, changes to its business operation, and other relevant circumstances, including the heightened cyber-attack risk environment.

64. Defendant violated the GLBA and its own policies and procedures by sharing the PII of Plaintiff and Class Members with a non-affiliated third party without providing Plaintiff and Class Members (a) an opt-out notice; and (b) a reasonable opportunity to opt out of such disclosure.

65. Defendant has not informed Plaintiff and Class Members of the reason Defendant kept the PII of more than 1.5 million individuals on an unsecured platform, accessible from the internet, especially considering its recent breach in March 2021; if this was done to share the PII with yet another non-affiliated third party, Defendant would be further in breach of the GLBA and its own policy and procedures in failing to provide Plaintiff and Class Members an opt-out notice and a reasonable opportunity to opt out of such disclosure.

66. In a ruling that took effect in May, the Federal Deposit Insurance Corp. (FDIC), the Office of the Comptroller of the Currency (OCC), and the Federal Reserve (together, the "agencies") now require banks to notify their primary federal regulator within 36 hours of determining whether a "significant computer-security incident" could disrupt business or the stability of the financial sector, and requires banks to inform affected bank customers "as soon as possible," recognizing cyberattacks targeting the financial services industry "have increased in frequency and severity in recent years."[33] Defendant violated this ruling by delaying notifying its customers of the cyber-attack for six months after it occurred.

67. Further, federal agencies have issued recommendations and guidelines to help minimize the risks of a data breach for businesses holding sensitive data. For example, the Federal Trade Commission (FTC) has issued numerous guides for business highlighting the importance of reasonable data security practices, which should be factored into all business-related decision making.[34]

68. The FTC's publication Protecting Personal Information: A Guide for Business sets forth fundamental data security principles and practices for businesses

[33] https://www.bankingdive.com/news/36-hour-window-fed-fdic-occ-cybersecurity-technology-vendor/592275/ (last visited June 28, 2022); https://www.federalreserve.gov/newsevents/pressreleases/files/bcreg20211118a1.pdf (last visited June 28, 2022).
[34] https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf (last visited June 28, 2022).

to implement and follow as a means to protect sensitive data.35 Among other things, the guidelines note that businesses should (a) protect the personal customer information that they collect and store; (b) properly dispose of personal information that is no longer needed; (c) encrypt information stored on their computer networks; (d) understand their network's vulnerabilities; and (e) implement policies to correct security problems. The FTC guidelines further recommend that businesses use an intrusion detection system, monitor all incoming traffic for unusual activity, monitor for large amounts of data being transmitted from their system, and have a response plan ready in the event of a breach.[36]

69. Additionally, the FTC recommends that organizations limit access to sensitive data, require complex passwords to be used on networks, use industry-tested methods for security; monitor for suspicious activity on the network, and verify that third-party service providers have implemented reasonable security measures.[37] This is consistent with guidance provided by the FBI.

70. The FTC has brought enforcement actions against businesses for failing to reasonably protect customer information, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential

[35] https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal information.pdf (last visited June 28, 2022).
[36] *Id*.
[37] FTC, *Start With Security*, *supra* note 35.

consumer data as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.[38]

71. Flagstar was fully aware of its obligation to implement and use reasonable measures to protect the PII of its customers but failed to comply with these basic recommendations and guidelines that would have prevented this breach from occurring. Flagstar's failure to employ reasonable measures to protect against unauthorized access to patient information constitutes an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45.

The Impact of the Data Breach on Victims

72. Flagstar's failure to keep Plaintiff's and Class Members' PII secure has severe ramifications. Given the sensitive nature of the PII stolen in the Data Breach—names and Social Security numbers—hackers can commit identity theft, financial fraud, and other identity-related fraud against Plaintiff and Class Members now and into the indefinite future. As a result, Plaintiff has suffered injury and faced an imminent and substantial risk of further injury including identity theft and related cybercrimes due to the Data Breach.

[38] https://www.ftc.gov/news-events/media-resources/protecting-consumer-privacy/privacy-security-enforcement (last visited June 28, 2022).

73. The PII exposed in the Data Breach is highly coveted and valuable on underground markets as it can be used to commit identity theft and fraud. Malicious actors use PII to, among other things, gain access to consumers' bank accounts, social media, and credit cards. Malicious actors can also use consumers' PII to open new financial records, open new utility accounts, obtain medical treatment using victims' health insurance, file fraudulent tax returns, obtain government benefits, obtain government IDs, or create "synthetic identities." [39]

74. Further, malicious actors often wait months or years to use the PII obtained in data breaches, as victims often become complacent and less diligent in monitoring their accounts after a significant period has passed. These bad actors will also re-use stolen PII, meaning individuals can be the victims of several cybercrimes stemming from a single data breach.

75. Given the confirmed exfiltration of PII from Flagstar's systems, many victims of the Data Breach have likely already experienced significant harms as the result of the Data Breach, including, but not limited to, identity theft and fraud. Plaintiff and Class Members have also spent time, money, and effort dealing with the fallout of the Data Breach, including purchasing credit monitoring services,

[39] A criminal combines real and fake information to create a new "synthetic" identity, which is used to commit fraud.

reviewing financial and healthcare statements, checking credit reports, and spending time and effort searching for and responding to unauthorized activity.

76. It is no wonder then that identity theft exacts a severe emotional toll on its victims. The 2017 Identity Theft Resource Center survey evidences the emotional suffering experienced by victims of identity theft:

- 75% of respondents reported feeling severely distressed;
- 67% reported anxiety;
- 66% reported feelings of fear related to personal financial safety;
- 37% reported fearing for the financial safety of family members;
- 24% reported fear for their physical safety;
- 15.2% reported a relationship ended or was severely and negatively impacted by the identity theft; and
- 7% reported feeling suicidal.[40]

77. Identity theft can also exact a physical toll on its victims. The same survey reported that respondents experienced physical symptoms stemming from their experience with identity theft:

- 48.3% of respondents reported sleep disturbances;
- 37.1% reported an inability to concentrate/lack of focus;
- 28.7% reported they were unable to go to work because of physical symptoms;

[40] https://www.idtheftcenter.org/images/page-docs/Aftermath_2017.pdf (last visited January 7, 2022).

- 23.1% reported new physical illnesses (aches and pains, heart palpitations, sweating, stomach issues); and
- 12.6% reported a start or relapse into unhealthy or addictive behaviors.[41]

78. The unauthorized disclosure of sensitive PII to data thieves also reduces its inherent value to its owner, which has been recognized by courts as an independent form of harm.[42]

79. Consumers are injured every time their data is stolen and traded on underground markets, even if they have been victims of previous data breaches. Indeed, the dark web is comprised of multiple discrete repositories of stolen information that can be aggregated together or accessed by different criminal actors who intend to use it for different fraudulent purposes. Each data breach increases the likelihood that a victim's personal information will be exposed to more individuals who are seeking to misuse it at the victim's expense.

80. As the result of the wide variety of injuries that can be traced to the Data Breach, Plaintiff and Class Members have and will continue to suffer economic

[41] *Id.*

[42] *See In re Marriott Int'l, Inc., Customer Data Sec. Breach Litig.*, 440 F. Supp. 3d 447, 462 (D. Md. 2020) ("Neither should the Court ignore what common sense compels it to acknowledge—the value that personal identifying information has in our increasingly digital economy. Many companies, like Marriott, collect personal information. Consumers too recognize the value of their personal information and offer it in exchange for goods and services.").

loss and other actual harm for which they are entitled to damages, including, but not limited to, the following:

a. the unconsented disclosure of confidential information to a third party;

b. losing the inherent value of their PII;

c. losing the value of the explicit and implicit promises of data security;

d. identity theft and fraud resulting from the theft of their PII;

e. costs associated with the detection and prevention of identity theft and unauthorized use of their financial accounts;

f. anxiety, emotional distress, and loss of privacy;

g. costs associated with purchasing credit monitoring, credit freezes, and identity theft protection services;

h. unauthorized charges and loss of use of and access to their financial and investment account funds and costs associated with inability to obtain money from their accounts or being limited in the amount of money they were permitted to obtain from their accounts, including missed payments on bills and loans, late charges and fees, and adverse effects on their credit;

i. lowered credit scores resulting from credit inquiries following fraudulent activities;

j. costs associated with time spent and the loss of productivity or the enjoyment of one's life from taking time to address and attempt to mitigate and address the actual and future consequences of the Data Breach, including searching for fraudulent activity, imposing withdrawal and purchase limits on compromised accounts, and the stress, nuisance, and annoyance of dealing with the repercussions of the Data Breach; and

k. the continued, imminent, and certainly impending injury flowing from potential fraud and identify theft posed by their PII being in the possession of one or many unauthorized third parties.

81. Even in instances where an individual is reimbursed for a financial loss due to identity theft or fraud, that does not make that individual whole again as there is typically significant time and effort associated with seeking reimbursement.

82. There may also be a significant time lag between when personal information is stolen and when it is misused for fraudulent purposes. According to the Government Accountability Office, which conducted a study regarding data breaches: "law enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm."[43]

83. Plaintiff and Class Members place significant value in data security. According to a survey conducted by cyber-security company FireEye Mandiant, approximately 50% of consumers consider data security to be a main or important consideration when making purchasing decisions and nearly the same percentage would be willing to pay more to work with a provider that has better data security. 70% of consumers would provide less personal information to organizations that suffered a data breach.[44]

[43] http://www.gao.gov/new.items/d07737.pdf (last visited June 28, 2022).
[44] https://www.fireeye.com/blog/executive-perspective/2016/05/beyond_the_bottomli.html (last visited June 28, 2022).

84. Likewise, the American Bankers Association, reporting on a global consumer survey regarding concerns about privacy and data security, noted that 29% of consumers would avoid using a company that had experienced a data breach, with 63% of consumers indicating they would avoid such a company for a period of time.[45]

85. According to another survey conducted by KRC Research for credit reporting company Experian, consumers expect a faster response from their bank after a data breach than other companies.[46] Sixty-six percent of people surveyed said they would stop doing business with a company that had a slow or ineffective response to a data breach and would switch to a competitor. Forty-five percent said they would tell their family or friends to stop doing business with the company. The survey also "suggests financial services companies have more to lose—both in reputation and customer base—than do other businesses." Eighty-three percent of respondents said they expected to be notified within 24 hours if the breached company is a bank.[47]

86. Because of the value consumers place on data privacy and security, financial services providers with robust data security practices are viewed more

[45] https://bankingjournal.aba.com/2019/09/what-compliance-needs-to-know-in-the-event-of-a-security-breach/ (last visited June 28, 2022).
[46] Banks have more to lose from data breaches than other companies | Banking Dive (last visited June 28, 2022).
[47] *Id.*

favorably by consumers and can command higher prices than those who do not. Consequently, had Flagstar's customers known the truth about its data security practices—that the organization did not adequately protect and store their PII—they would not have sought financial services from Flagstar or would have paid significantly less. As such, Plaintiff and Class Members did not receive the benefit of their bargain with Flagstar because they paid for the value of services they did not receive.

87. Plaintiff and Class Members have a direct interest in Flagstar's promises and duties to protect their PII, *i.e.*, that Flagstar *not increase* their risk of identity theft and fraud. Because Flagstar failed to live up to its promises and duties in this respect, Plaintiff and Class Members seek the present value of identity protection services to compensate them for the present harm and present and continuing increased risk of harm caused by Flagstar's wrongful conduct. Through this remedy, Plaintiff seeks to restore himself and Class Members as close to the same position as they would have occupied but for Flagstar's wrongful conduct, namely its failure to adequately protect Plaintiff's and Class Members' PII.

88. Plaintiff and Class Members further seek to recover the value of the unauthorized access to their PII permitted through Flagstar's wrongful conduct. This measure of damages is analogous to the remedies for unauthorized use of intellectual property. Like a technology covered by a trade secret or patent, use or access to a

person's PII is non-rivalrous—the unauthorized use by another does not diminish the rights-holder's ability to practice the patented invention or use the trade-secret protected technology. Nevertheless, a plaintiff may generally recover the reasonable use value of the IP—*i.e.*, a "reasonable royalty" from an infringer. This is true even though the infringer's use did not interfere with the owner's own use (as in the case of a non-practicing patentee) and even though the owner would not have otherwise licensed such IP to the infringer. A similar royalty or license measure of damages is appropriate here under common law damages principles authorizing recovery of rental or use value. This measure is appropriate because (a) Plaintiff and Class Members have a protectible property interest in their PII; (b) the minimum damages measure for the unauthorized use of personal property is its rental value; and (c) rental value is established with reference to market value, *i.e.*, evidence regarding the value of similar transactions.

89. Flagstar's delayed notice letter also caused Plaintiff and Class Members harm. For example, Flagstar provided no context for its repeated unsubstantiated statement that there was "no evidence that any of your information has been misused" as the objective of almost every data breach is to gain access to an organization's sensitive data so that the data can be misused for financial gain. Furthermore, the letter did not explain the precise nature of the attack, the identity of the hackers, or the number of individuals affected. Flagstar's decision to withhold

these key facts is significant because affected individuals may take different precautions depending on the severity and imminence of the perceived risk. By waiting months to disclose the Data Breach and by downplaying the risk of misuse, Flagstar prevented victims from taking meaningful, proactive, and targeted mitigation measures to secure their financial data and bank accounts.

90. Because Flagstar continues to hold the PII of its customers and employees, Plaintiff and Class Members have an interest in ensuring that their PII is secured and not subject to further theft.

CLASS ACTION ALLEGATIONS

NATIONWIDE CLASS

91. Pursuant to Fed. R. Civ. P. 23(b)(2) and (b)(3), as applicable, and (c)(4), Plaintiff seeks certification of the following nationwide class (the "Nationwide Class" or the "Class"):

> **All individuals residing in the United States whose PII was compromised in the Data Breach.**

92. The Nationwide Class asserts claims against Flagstar for negligence (Count I), breach of implied contract (Count II), negligence *per se* (Count III), unjust enrichment (Count IV), breach of confidence (Count V), invasion of privacy—intrusion upon seclusion (Count VI).

CALIFORNIA SUBCLASS

93. Pursuant to Fed. R. Civ. P. 23(b)(2) and (b)(3), as applicable, and (c)(4), Plaintiff seeks certification of state-by-state claims in the alternative to the nationwide claims, as well as statutory claims under state data breach statutes and consumer protection statutes (Counts VII through IX), on behalf of a separate statewide Subclass for California (the "Subclass" or "California Subclass"), defined as follows:

> **All individuals residing in California whose PII was compromised in the Data Breach.**

94. Specifically excluded from the Nationwide Class and the Subclass are Defendant; its officers, directors, or employees; any entity in which Defendant has a controlling interest; and any affiliate, legal representative, heir, or assign of Defendant. Also excluded from the Class are any federal, state, or local governmental entities, any judicial officer presiding over this action and the members of their immediate family and judicial staff, and any juror assigned to this action.

95. **Ascertainablity.** The members of the Class and Subclass are readily identifiable and ascertainable. Defendant and/or its affiliates, among others, possess the information to identify and contact Class Members.

96. **Numerosity: Federal Rule of Civil Procedure 23(a)(1).** The members of the Class and Subclass are so numerous that joinder of all of them is impracticable.

Flagstar's disclosures reveal that the Class contains more than 1.5 million individuals whose PII was compromised in the Data Breach.

97. **Typicality: Federal Rule of Civil Procedure 23(a)(3).** As to the Class and Subclass, Plaintiff's claims are typical of the claims of the members because all Class Members had their PII compromised in the Data Breach and were harmed as a result.

98. **Adequacy of Representation: Federal Rule of Civil Procedure 23(a)(4).** Plaintiff will fairly and adequately protect the interests of the Class and Subclass. Plaintiff has no known interest antagonistic to those of the Class and their interests are aligned with Class Members' interests. Plaintiff was subject to the same Data Breach as Class Members, suffered similar harms, and face similar threats due to the Data Breach. Plaintiff has also retained competent counsel with significant experience litigating complex class actions, including Data Breach cases involving multiple classes and data breach claims.

99. **Commonality and Predominance: Federal Rule of Civil Procedure 23(a)(2) and 23(b)(3).** There are questions of law and fact common to the Class such that there is a well-defined community of interest in this litigation. These common questions predominate over any questions affecting only individual Class Members. The common questions of law and fact include, without limitation:

a. Whether Defendant owes Plaintiff and Class Members a duty to implement and maintain reasonable security procedures and practices to protect their PII;

b. Whether Defendant breached an agreement with Plaintiff and Class Members to keep their PII confidential;

c. Whether Defendant received a benefit without proper restitution making it unjust for Defendant to retain the benefit without commensurate compensation;

d. Whether Defendant acted negligently in connection with the monitoring and/or protection of Plaintiff's and Class Members' PII;

e. Whether Defendant violated its duty to implement reasonable security systems to protect Plaintiff's and Class Members' PII;

f. Whether Defendant's breach of its duty to implement reasonable security systems directly and/or proximately caused damages to Plaintiff and Class Members;

g. Whether Defendant provided timely notice of the Data Breach to Plaintiff and Class Members; and

h. Whether Class Members are entitled to compensatory damages, punitive damages, and/or statutory or civil penalties as a result of the Data Breach.

100. Defendant has engaged in a common course of conduct and Plaintiff and Class Members have been similarly impacted by Defendant's failure to maintain reasonable security procedures and practices to protect customer's PII, as well as Defendant's failure to timely alert affected customers to the Data Breach.

101. **Superiority: Federal Rule of Civil Procedure 23(b)(3).** A class action is superior to other available methods for the fair and efficient adjudication of the controversy. Class treatment of common questions of law and fact is superior to

multiple individual actions or piecemeal litigation. Absent a class action, most if not all Class Members would find the cost of litigating their individual claims prohibitively high and have no effective remedy. The prosecution of separate actions by individual Class Members would create a risk of inconsistent or varying adjudications with respect to individual Class Members and risk inconsistent treatment of claims arising from the same set of facts and occurrences. Plaintiff knows of no difficulty likely to be encountered in the maintenance of this action as a class action under the applicable rules.

CLAIMS FOR RELIEF

COUNT I
Negligence
(On Behalf of Plaintiff and the Nationwide Class, or in the alternative, Plaintiff and the California Subclass)

102. Plaintiff repeats and realleges every allegation set forth in the preceding paragraphs.

103. Defendant required Plaintiff and Class Members to provide their PII as a condition of receiving financial services. Defendant collected and stored the data for purposes of providing financial services as well as for commercial gain.

104. Defendant owed Plaintiff and Class Members a duty to exercise reasonable care in protecting their PII from unauthorized disclosure or access.

105. Defendant owed a duty of care to Plaintiff and Class Members to provide adequate data security, consistent with industry standards, to ensure that Defendant's systems and networks adequately protected the PII.

106. As a financial services provider, Defendant had a special relationship with Plaintiff and Class Members who entrusted Defendant to adequately their confidential personal and financial information.

107. Defendant's duty to use reasonable care in protecting PII arises as a result of the parties' relationship, as well as common law and federal law, and Defendant's own policies and promises regarding privacy and data security.

108. Defendant knew, or should have known, of the risks inherent in collecting and storing PII in a centralized location, Defendant's vulnerability to network attacks, and the importance of adequate security.

109. Defendant breached its duty to Plaintiff and Class Members in numerous ways, as described herein, including by:

a. Failing to exercise reasonable care and implement adequate security systems, protocols, and practices sufficient to protect the PII of Plaintiff and Class Members;

b. Failing to comply with industry standard data security measures for the financial industry leading up to the Data Breach;

c. Failing to adequately audit the data security practices of third parties who were granted access to Defendant's networks;

d. Failing to comply with its own Privacy Policy;

e. Failing to comply with regulations protecting the PII at issue during the period of the Data Breach;

f. Failing to adequately monitor, evaluate, and ensure the security of Defendant's network and systems;

g. Failing to recognize in a timely manner that PII had been compromised; and

h. Failing to timely and adequately disclose the Data Breach.

110. Plaintiff's and Class Members' PII would not have been compromised but for Defendant's wrongful and negligent breach of its duties.

111. Defendant's failure to take proper security measures to protect the sensitive PII of Plaintiff and Class Members created conditions conducive to a foreseeable, intentional criminal act, namely the unauthorized access and exfiltration of PII by unauthorized third parties. Given that financial services providers are prime targets for hackers, Plaintiff and Class Members are part of a foreseeable, discernible group that was at high risk of having their PII misused or disclosed if not adequately protected by Defendant.

112. It was also foreseeable that Defendant's failure to provide timely and forthright notice of the Data Breach would result in injury to Plaintiff and Class Members.

113. As a direct and proximate result of Defendant's conduct, Plaintiff and Class Members have and will suffer damages including: (i) the loss of rental or use value of their PII; (ii) the unconsented disclosure of their PII to unauthorized third parties; (iii) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, fraud, and/or unauthorized use of their PII; (iv) lost opportunity costs associated with addressing and attempting to mitigate the actual and future consequences of the Data Breach, including, but not limited to, efforts spent researching how to prevent, detect, contest, and recover from fraud and identity theft; (v) time, effort, and expense associated with placing fraud alerts or freezes on credit reports; (vi) anxiety, emotional distress, loss of privacy, and other economic and non-economic losses; (vii) the continued risk to their PII, which remains in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect it; (viii) future costs in terms of time, effort and money that will be expended to prevent, detect, contest, and repair the inevitable and continuing consequences of compromised PII for the rest of their lives; and (ix) any nominal damages that may be awarded.

COUNT II
Breach of Implied Contract
(On Behalf of Plaintiff and the Nationwide Class, or in the alternative, Plaintiff and the California Subclass)

114. Plaintiff repeats and realleges every allegation set forth in the preceding paragraphs.

115. Plaintiff and Class Members were required to provide their PII to Defendant in order to receive financial services.

116. As part of these transactions, Defendant agreed to safeguard and protect the PII of Plaintiff and Class Members. Implicit in these transactions between Defendant and Class Members was the obligation that Defendant would use the PII for approved business purposes only and would not make unauthorized disclosures of the information or allow unauthorized access to the information.

117. Additionally, Defendant implicitly promised to retain this PII only under conditions that kept such information secure and confidential and therefore had a duty to reasonably safeguard and protect the PII of Plaintiff and Class Members from unauthorized disclosure or access.

118. Plaintiff and Class Members entered into implied contracts with the reasonable expectation that Defendant's data security practices and policies were reasonable and consistent with industry standards. Plaintiff and Class Members believed that Defendant would use part of the monies paid to Defendant under the

implied contracts to fund adequate and reasonable data security practices to protect their PII.

119. Plaintiff and Class Members would not have provided and entrusted their PII to Defendant or would have paid less for Defendant's services in the absence of the implied contract between them and Defendant. The safeguarding of Plaintiff's and Class Members' PII was critical to realizing the intent of the parties.

120. The nature of Defendant's implied promise itself—the subject matter of the contractual provision at issue—was to protect Plaintiff's and Class Members' PII in order to prevent harm and prevent present and continuing increased risk.

121. Defendant breached its implied contract with Plaintiff and Class Members by failing to reasonably safeguard and protect their PII, which was compromised as a result of the Data Breach.

122. As a direct and proximate result of Defendant's breaches, Plaintiff and Class Members sustained actual losses and damages as alleged herein, including that they did not receive the benefits of the bargains for which they paid. Plaintiff and Class Members alternatively seek an award of nominal damages.

COUNT III
Negligence *Per Se*
(On Behalf of Plaintiff and the Nationwide Class, or in the alternative, Plaintiff and the California Subclass)

123. Plaintiff repeats and realleges every allegation set forth in the preceding paragraphs.

124. Section 5 of the Federal Trade Commission Act ("FTC Act") prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such as Defendant, of failing to use reasonable measures to protect PII. 15 U.S.C. § 45(a)(1).

125. The FTC publications and orders described above also form part of the basis of Defendant's duty in this regard.

126. Defendant violated Section 5 of the FTC Act by failing to use reasonable measures to protect PII and failing to comply with applicable industry standards. Defendant's conduct was unreasonable given the nature and amount of PII they obtained, stored, and disseminated in the regular course of their business, and the foreseeable consequences of a data breach, including, specifically, the significant damage that would result to Plaintiff and Class Members.

127. Defendant's violations of Section 5 of the FTC Act constitute negligence *per se*.

128. Defendant violated the GLBA, its Privacy Rule and/or Regulation P, and its Safeguards Rule by, among other things: (a) failing to provide annual privacy notices to customers after the customer relationship ended, despite retaining these customers' PII and storing and/or sharing that PII on Defendant's internal systems that were inadequately secured and accessible to unauthorized third-parties from the internet; (b) failing to adequately inform its customers that it was storing and/or

sharing, or would store and/or share, the customers' PII on such an insecure platform and/or system; (c) failing to assess reasonably foreseeable risks to the security, confidentiality, and integrity of customer information; (d) failing to adequately (i) test and/or monitor the system were the Data Breach occurred and (ii) update and/or further secure its data security practices in light of the heightened risk environment; and (e) failing to send opt-out notices and afford a reasonable opportunity to opt out of disclosures before sharing the PII of more than 1.5 million individuals with one or more non-affiliated third parties.

129. Defendant's violation of the GLBA, its Privacy Rule and/or Regulation P, and its Safeguards Rule constitutes *negligence per se*.

130. Plaintiff and Class Members are within the class of persons that the FTC Act and the GLBA were intended to protect.

131. The harm that occurred as a result of the Data Breach is the type of harm the FTC Act was intended to guard against. The FTC has pursued enforcement actions against businesses, which, as a result of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm as that suffered by Plaintiff and Class Members. The GLBA, with its Privacy Rule, Regulation P, and Safeguards Rule, was similarly intended to guard against harms such as the harm that occurred as a result of the Data Breach.

132. As a direct and proximate result of Defendant's negligence *per se*, Plaintiff and Class Members sustained actual losses and damages as alleged herein.

COUNT IV
Unjust Enrichment
(On Behalf of Plaintiff and the Nationwide Class, or in the alternative, Plaintiff and the California Subclass)

133. Plaintiff repeats and realleges every allegation set forth in the preceding paragraphs.

134. Plaintiff and Class Members have an interest, both equitable and legal, in their PII that was conferred upon, collected by, and maintained by Defendant and which was stolen in the Data Breach. This information has independent value.

135. Plaintiff and Class Members conferred a monetary benefit on Defendant in the form of payments for financial services, including those paid indirectly by Plaintiff and Class Members to Defendant.

136. Defendant appreciated and had knowledge of the benefits conferred upon it by Plaintiff and Class Members.

137. The price for financial services that Plaintiff and Class Members paid (directly or indirectly) to Defendant should have been used by Defendant, in part, to pay for the administrative costs of reasonable data privacy and security practices and procedures.

138. Likewise, in exchange for receiving Plaintiff's and Class Members' valuable PII, which Defendant was able to use for their own business purposes and

which provided actual value to Defendant, Defendant was obligated to devote sufficient resources to reasonable data privacy and security practices and procedures.

139. As a result of Defendant's conduct, Plaintiff and Class Members suffered actual damages as described herein. Under principals of equity and good conscience, Defendant should be compelled to disgorge into a common fund for the benefit of Plaintiff and Class Members all unlawful or inequitable proceeds they received from Plaintiff and Class Members, including damages equaling the difference in value between financial services that included implementation of reasonable data privacy and security practices that Plaintiff and Class Members paid for and the services without reasonable data privacy and security practices that they actually received.

COUNT V
Breach of Confidence
(On Behalf of Plaintiff and the Nationwide Class, or in the alternative, Plaintiff and the California Subclass)

140. Plaintiff repeats and realleges every allegation set forth in the preceding paragraphs.

141. Plaintiff and Class Members maintained a confidential relationship with Defendant whereby Defendant undertook a duty not to disclose PII provided by Plaintiff and Class Members to unauthorized third parties. Such PII was confidential and novel, highly personal and sensitive, and not generally known.

142. Defendant knew Plaintiff's and Class Members' PII was being disclosed in confidence and understood the confidence was to be maintained, including by expressly and implicitly agreed to protect the confidentiality and security of the PII it collected, stored, and maintained.

143. There was disclosure of Plaintiff's and Class Members' PII as a result of the Data Breach in violation of this understanding. The disclosure occurred because Defendant failed to implement and maintain reasonable safeguards to protect its customers' PII and failed to comply with industry-standard data security practices.

144. Plaintiff and Class Members were harmed the moment an unconsented disclosure of their confidential information occurred.

145. As a direct and proximate result of Defendant's breach of confidence, Plaintiff and Class Members suffered injury and sustained actual losses and damages as alleged herein. Plaintiff and Class Members alternatively seek an award of nominal damages.

COUNT VI
Invasion of Privacy—Intrusion Upon Seclusion
(On Behalf of Plaintiff and the Nationwide Class, or in the alternative, Plaintiff and the California Subclass)

146. Plaintiff repeats and realleges every allegation set forth in the preceding paragraphs.

147. Plaintiff and Class Members shared PII with Flagstar that Plaintiff and Class Members wanted to remain private and non-public.

148. Plaintiff and Class Members reasonably expected that the PII he shared with Flagstar would be protected and secured against access by unauthorized parties and would not be disclosed to or obtained by unauthorized parties, or disclosed or obtained for any improper purpose.

149. Flagstar intentionally intruded into Plaintiff's and Class Members' seclusion by disclosing without permission their PII to a third party who then sold their PII to other third-parties on the dark web.

150. By failing to keep Plaintiff's and Class Members' PII secure, and disclosing PII to unauthorized parties for unauthorized use, Flagstar unlawfully invaded Plaintiff's and Class Members' privacy right to seclusion by, inter alia:

a. Intruding into their private affairs in a manner that would be highly offensive to a reasonable person;

b. Invading their privacy by improperly using their PII properly obtained for another purpose, or disclosing it to unauthorized persons;

c. Failing to adequately secure their PII from disclosure to unauthorized persons; and

d. Enabling the disclosures of their PII without consent.

151. The PII that was publicized during the Data Breach was highly sensitive, private, and confidential, as it included private financial and other PII.

152. Flagstar's intrusions into Plaintiff's and Class Members' seclusion were substantial and would be highly offensive to a reasonable person, constituting an egregious breach of social norms.

153. As a direct and proximate result of Defendant's invasion of privacy, Plaintiff and Class Members suffered injury and sustained actual losses and damages as alleged herein. Plaintiff and Class Members alternatively seek an award of nominal damages.

COUNT VII
California Consumer Privacy Act ("CCPA"),
Cal. Civ. Code §§ 1798.150, *et seq.*
(On Behalf of Plaintiff and the California Subclass)

154. Plaintiff, individually and on behalf of the California Subclass, repeats and realleges the allegations set forth in the preceding paragraphs as if fully set forth herein.

155. Plaintiff and the California Subclass Members are residents of California.

156. Flagstar is a corporation organized or operated for the profit or financial benefit of its owners with annual gross revenues over $1.6 billion. Defendant collects customers' personal information as defined in Cal. Civ. Code § 1798.140.

157. Flagstar violated § 1798.150 of the CCPA by failing to prevent Plaintiff's and the California Subclass Members' nonencrypted PII from unauthorized access and exfiltration, theft, or disclosure as a result of Flagstar's violations of its duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information.

158. Flagstar has a duty to implement and maintain reasonable security procedures and practices to protect Plaintiff's and the California Subclass Members' PII. As detailed herein, Flagstar failed to do so.

159. As a direct and proximate result of Flagstar's acts, Plaintiff's and the California Subclass Members' PII, including Social Security numbers and names, was subjected to unauthorized access and exfiltration, theft, or disclosure.

160. Plaintiff and the California Subclass Members seek injunctive or other equitable relief to ensure Flagstar hereinafter adequately safeguards customers' PII by implementing reasonable security procedures and practices. Such relief is particularly important Flagstar continues to hold customers' PII, including Plaintiff's and the California Subclass Members' PII. Plaintiff and the California Subclass Members have an interest in ensuring that their PII is reasonably protected, and Flagstar has demonstrated a pattern of failing to adequately safeguard this information, as evidenced by its multiple data breaches.

161. Pursuant to Cal. Civ. Code § 1798.150(b), Plaintiff will mail a CCPA notice letter to Defendant's registered service agent, detailing the specific provisions of the CCPA that Flagstar has and continues to violate. If Defendant cannot cure within 30 days, which Plaintiff believes is not possible given that the harm has already occurred, then Plaintiff intends to amend the Complaint to seek statutory damages as permitted by the CCPA individually and on behalf of the California Subclass Members.

162. As described herein, an actual controversy has arisen and now exists as to whether Defendant implemented and maintained reasonable security procedures and practices appropriate to the nature of the information to protect the PII under the CCPA.

COUNT VIII
California Customer Records Act
Cal. Civ. Code §§ 1798.80, *et seq.*
(On Behalf of Plaintiff and the California Subclass)

163. Plaintiff, individually and on behalf of the California Subclass, repeats and realleges the allegations set forth in the preceding paragraphs as if fully set forth herein.

164. "[T]o ensure that personal information about California residents is protected," the California legislature enacted Cal. Civ. Code § 1798.81.5, which requires that any business that "owns, licenses, or maintains personal information about a California resident shall implement and maintain reasonable security

procedures and practices appropriate to the nature of the information, to protect the PII from unauthorized access, destruction, use, modification, or disclosure."

165. Flagstar is a business that owns, maintains, and licenses personal information, within the meaning of Cal. Civ. Code § 1798.81.5, about Plaintiff and the California Subclass Members.

166. Businesses that own or license computerized data that includes PII, including Social Security numbers, are required to notify California residents when their PII has been acquired (or is reasonably believed to have been acquired) by unauthorized persons in a data security breach "in the most expedient time possible and without unreasonable delay." Cal. Civ. Code § 1798.82. Among other requirements, the security breach notification must include "the types of PII that were or are reasonably believed to have been the subject of the breach." Cal. Civ. Code § 1798.82.

167. Flagstar is a business that owns or licenses computerized data that includes PII as defined by Cal. Civ. Code § 1798.82.

168. Plaintiff's and the California Subclass Members' PII (e.g., Social Security numbers) includes PII as covered by Cal. Civ. Code § 1798.82.

169. Because Flagstar reasonably believed that Plaintiff's and the California Subclass Members' PII was acquired by unauthorized persons during the Flagstar

data breach, Flagstar had an obligation to disclose the data breach in a timely and accurate fashion as mandated by Cal. Civ. Code § 1798.82.

170. Flagstar failed to fully disclose material information about the Data Breach in a timely fashion.

171. By failing to disclose the data breach in a timely and accurate manner, Flagstar violated Cal. Civ. Code § 1798.82.

172. As a direct and proximate result of Flagstar's violations of the Cal. Civ. Code §§ 1798.81.5 and 1798.82, Plaintiff and the California Subclass Members suffered damages, as described above.

173. Plaintiff and the California Subclass Members seek relief under Cal. Civ. Code § 1798.84, including actual damages and injunctive relief.

COUNT IX
California Unfair Competition Act
Cal. Bus. & Prof. Code §§ 17200, *et seq.*
(On Behalf of Plaintiff and the California Subclass)

174. Plaintiff, individually and on behalf of the California Subclass, repeats and realleges the allegations set forth in the preceding paragraphs as if fully set forth herein.

175. Flagstar is a "person" as defined by Cal. Bus. & Prof. Code §17201.

176. Flagstar violated Cal. Bus. & Prof. Code §§ 17200, et seq. ("UCL") by engaging in unlawful, unfair, and deceptive business acts and practices.

177. Flagstar's "unfair" acts and practices include:

a. Flagstar failed to implement and maintain reasonable security measures to protect Plaintiff's and the California Subclass Members' PII from unauthorized disclosure, release, data breaches, and theft, which was a direct and proximate cause of the Data Breach.

b. Flagstar failed to identify foreseeable security risks, remediate identified security risks, and adequately improve security following previous cybersecurity incidents, as described herein. This conduct, with little if any utility, is unfair when weighed against the harm to Plaintiff and the California Subclass Members, whose PII has been compromised.

c. Flagstar's failure to implement and maintain reasonable security measures also was contrary to legislatively-declared public policy that seeks to protect consumers' data and ensure that entities that are trusted with it use appropriate security measures. These policies are reflected in laws, including the FTC Act, 15 U.S.C. § 45; the GLBA, its Privacy Rule and/or Regulation P, and its Safeguards Rule; California's Consumer Records Act, Cal. Civ. Code § 1798.81.5; and California's Consumer Privacy Act, Cal. Civ. Code § 1798.100.

d. Flagstar's failure to implement and maintain reasonable security measures also resulted in substantial consumer injuries, as described

above, that are not outweighed by any countervailing benefits to consumers or competition. Moreover, because consumers could not know of Flagstar's grossly inadequate security, Flagstar's customers could not have reasonably avoided the harms that Flagstar caused.

e. Flagstar engaged in unlawful business practices by violating Cal. Civ. Code § 1798.82.

f. Flagstar has engaged in "unlawful" business practices by violating multiple laws, including California's Consumer Records Act, Cal. Civ. Code §§ 1798.81.5 (requiring reasonable data security measures) and 1798.82 (requiring timely breach notification); California's Consumers Legal Remedies Act, Cal. Civ. Code §§ 1780, *et seq.*; the FTC Act, 15 U.S.C. § 45; the GLBA, its Privacy Rule and/or Regulation P, and its Safeguards Rule; and California common law.

178. Flagstar's unlawful, unfair, and deceptive acts and practices include:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff's and the California Subclass Members' PII, which was a direct and proximate cause of the Data Breach;

b. Failing to identify and remediate foreseeable security and privacy risks and adequately improve security and privacy measures despite

knowing the risk of cybersecurity incidents, which was a direct and proximate cause of the Data Breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and the California Subclass Members' PII, including duties imposed by the FTC Act (15 U.S.C. § 45); and the GLBA, its Privacy Rule and/or Regulation P, and its Safeguards Rule, which was a direct and proximate cause of the Data Breach;

d. Misrepresenting that they would protect the privacy and confidentiality of Plaintiff's and the California Subclass Members' PII, including by implementing and maintaining reasonable security measures;

e. Misrepresenting that they would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and the California Subclass Members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45 and the GLBA, its Privacy Rule and/or Regulation P, and its Safeguards Rule;

f. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff's and the California Subclass Members' PII; and

g. Omitting, suppressing, and concealing the material fact that they did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and the California Subclass Members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45; the GLBA, its Privacy Rule and/or Regulation P, and its Safeguards Rule; California's Consumer Privacy Act, Cal. Civ. Code § 1798.100; California's Consumer Records Act, Cal. Civ. Code §§ 1798.80, *et seq.* and 1798.81.5, which was a direct and proximate cause of the Data Breach.

179. Flagstar's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Flagstar's data security and ability to protect the confidentiality of consumers' PII.

180. As a direct and proximate result of Flagstar's unfair, unlawful, and fraudulent acts and practices, Plaintiff and the California Subclass Members were injured and suffered monetary and non-monetary damages, as described herein, including but not limited to fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; loss of value of their PII; overpayment for Flagstar's services; loss of the value of access to their PII; and the value of identity protection services made necessary by the Data Breach.

181. Flagstar acted intentionally, knowingly, and maliciously to violate California's Unfair Competition Law, and recklessly disregarded Plaintiff's and the California Subclass Members' rights. Flagstar's past data breaches put it on notice that its security and privacy protections were inadequate.

182. Plaintiff and the California Subclass Members seek all monetary and non-monetary relief allowed by law, including restitution of all profits stemming from Flagstar's unfair, unlawful, and fraudulent business practices or use of their PII; declaratory relief; reasonable attorneys' fees and costs under California Code of Civil Procedure § 1021.5; injunctive relief; and other appropriate equitable relief.

REQUEST FOR RELIEF

WHEREFORE, Plaintiff, on behalf of himself and the Class and Subclass set forth herein, respectfully requests the following relief:

A. That the Court certify this action as a class action and appoint Plaintiff and their Counsel to represent the Class and Subclass;

B. That the Court grant permanent injunctive relief to prohibit and prevent Defendant from continuing to engage in the unlawful acts, omissions, and practices described herein;

C. That the Court award Plaintiff and Class Members compensatory, consequential, and general damages, including nominal damages as appropriate, for each count as allowed by law in an amount to be determined at trial;

D. That the Court award statutory damages, trebled, nominal, and/or punitive or exemplary damages, to the extent permitted by law;

E. That the Court order disgorgement and restitution of all earnings, profits, compensation, and benefits received by Defendant as a result of their unlawful acts, omissions, and practices;

F. That Plaintiff be granted the declaratory and injunctive relief sought herein;

G. That the Court award to Plaintiff the costs and disbursements of the action, along with reasonable attorneys' fees, costs, and expenses; and

H. That the Court award pre-and post-judgment interest at the maximum legal rate and all such other relief as it deems just and proper.

DEMAND FOR JURY TRIAL

Plaintiff hereby demand a jury trial in the instant action.

Dated: June 29, 2022

/s/ *Michael N. Hanna*
Michael N. Hanna (P81462)
MORGAN & MORGAN, P.A.
2000 Town Center, Suite 1900
Southfield, MI 48075
(313) 251-1399
mhanna@forthepeople.com

Norman E. Siegel*
Austin Moore*
Jordan A. Kane*
STUEVE SIEGEL HANSON LLP
460 Nichols Road, Suite 200
Kansas City, Missouri 64112
Telephone: (816) 714-7100
siegel@stuevesiegel.com
moore@stuevesiegel.com
kane@stuevesiegel.com
**Pro Hac Vice Forthcoming*

Counsel for Plaintiff and the Class